

Projekt 0.7. Vinklens tredeling – fra græsk geometri til moderne algebra

1. Elementære konstruktioner – de fire regningsarter udført med passer og lineal . 2	
Konstruktion af $a + b$ og af $a - b$ (hvis $a > b$).....2	2
Konstruktion af $a \cdot b$ (konstruktion af »fjerdeproportionalen«)2	2
Konstruktion af $\frac{a}{b}$2	2
2. Konstruktion af kvadratrødder med passer og lineal 3	3
3. Tredelingskonstruktioner 3	3
4. Archimedes tredeling af vinklen 3	3
5. Oversættelse af vinkeltredeling til løsning af tredjegradslikning 4	4
6. Konstruerbare punkter – konstruerbare tal 6	6
6.1 Forudsætninger6	6
6.1.1 Tilladte konstruktioner med passer og lineal6	6
6.2 Konstruktion af de konstruerbare punkter7	7
7. Tallegemer..... 8	8
8. Beskrivelse af de konstruerbare tal..... 11	11
9. Tredeling af en vilkårlig vinkel er ikke mulig..... 14	14
10. Litteraturliste 18	18
11. Tillæg. Om Galois’ korte liv og bratte død 19	19

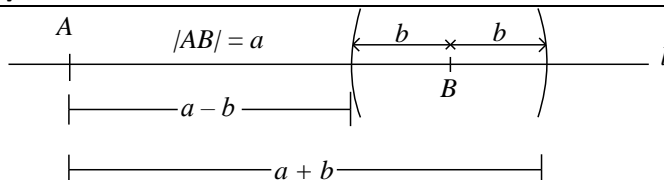
1. Elementære konstruktioner – de fire regningsarter udført med passer og lineal

(Dette afsnit indgår i HEM1, projekt 10.3 om Terningens fordobling, hvor det yderligere er udbygget med uddragning af kvadratrødder. Hvis du er fortrolig med, hvorledes man i geometrisk algebra opererer med de fire regningsarter +, −, · og /, så springer du bare kapitel 1 over.)

Lad være givet to positive tal a og b , $b \neq 0$, der begge repræsenteres af linjestykker med længderne a og b . Og lad endvidere være givet et linjestykke af længden 1.

Konstruktion af $a + b$ og af $a - b$ (hvis $a > b$)

Forlæng linjestykket a i en ret linje og tegn med centrum i et af a 's endepunkter en cirkel med radius b . Herved afskæres henholdsvis $a + b$ og $a - b$ på linjen:



Konstruktion af $a \cdot b$ (konstruktion af »fjerdeproportionalen«)

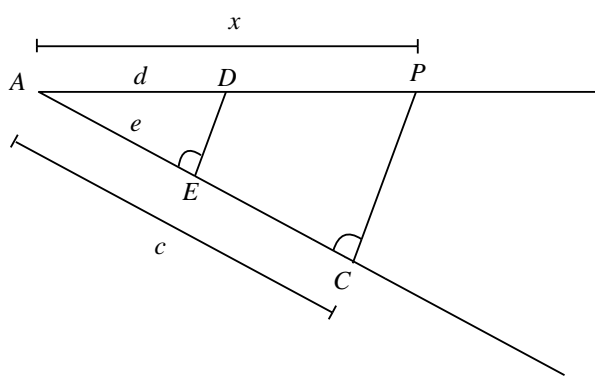
Konstruktionen bygger på følgende forhold: $\frac{a \cdot b}{b} = \frac{a}{1}$

Sæt $a \cdot b = x$. Opgaven er en speciel udgave af den generelle konstruktion af **fjerdeproportionalen** x til tre kendte stykker c , d og e :

$$\frac{x}{c} = \frac{d}{e}$$

Det gøres som følger:

Afsæt i en vilkårlig vinkel stykket d ud ad det ene ben og e ud ad det andet. Forbind DE . Afsæt c ud ad samme ben som e , og tegn igennem punktet C en linje parallel med DE .



Øvelse 2

Gør det! – dvs. flyt vinklen $\sphericalangle AED$ ned i C (ved brug af ”passer og lineal”, som man kan i et værktøjsprogram).

Nu er de to trekanter AED og ACP ensvinklede, og derfor gælder det ønskede:

$$\frac{x}{c} = \frac{d}{e}$$

Øvelse 3

Udfør nu selv konstruktionen af $a \cdot b$.

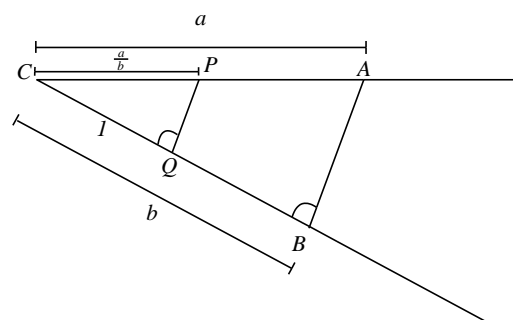
Konstruktion af $\frac{a}{b}$

Konstruktionen bygger på følgende forhold: $\frac{a}{b} = \frac{a}{b} \cdot \frac{1}{1}$

og udnytter metoden til konstruktion af fjerdeproportionalen,

hvor $x = \frac{a}{b}$:

Trekant ABC er ensvinklet med trekant PQC , deraf det ønskede.

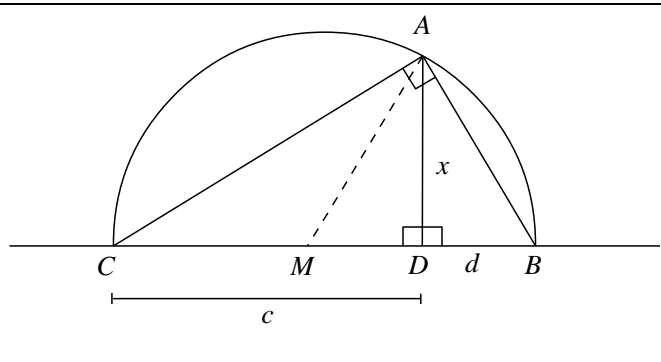


2. Konstruktion af kvadratrødder med passer og lineal

Konstruktionen af kvadratrødder er en speciel variant af den generelle konstruktion af **mellemproportionaler**:

$$\frac{x}{c} = \frac{d}{x}$$

Afsæt c og d i forlængelse af hinanden ud ad en ret linje, find midtpunktet M af dette linjestykke, og tegn med M som centrum og afstanden MC som radius en halvcirkel over CB . Oprejs i D den vinkelrette på linjen, og kald skæringspunktet med halvcirklen for A :



Øvelse 4

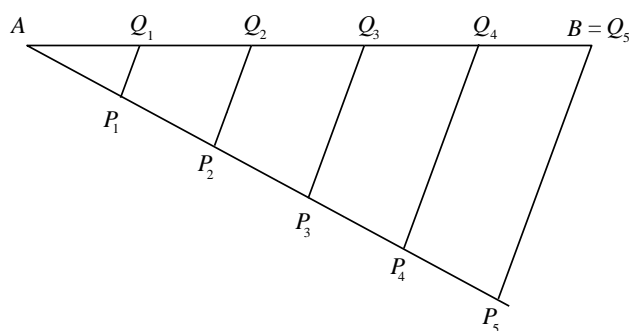
- Vis at trekanterne ABD og CAD er ensvinklede.
- Vis at $\frac{x}{c} = \frac{d}{x}$
- Argumenter for, at stykket DA bliver lig med $\sqrt{c \cdot d}$.

Øvelse 5

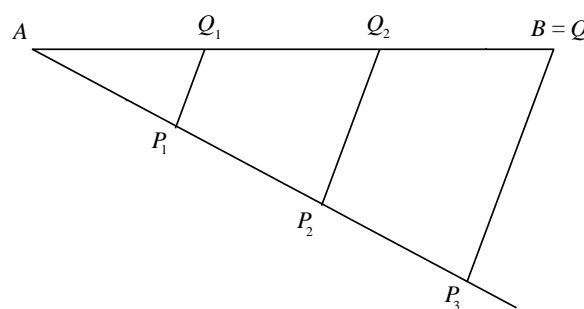
Anvend metoden ovenfor til at konstruere $\sqrt{3}$ og $\sqrt{2}$, idet du udnytter at $3 = 3 \cdot 1$ osv.

3. Tredelingskonstruktioner

Det er let at tredele et linjestykke. Eller for den sags skyld dele det op i n lige store dele, hvor $n \in \mathbb{N}$: Afsæt en vilkårlig vinkel, hvor linjen $l = AB$ ligger ud af det ene ben. Afsæt n lige lange stykker ned af det andet ben, så vi her får punkterne $P_1, P_2, P_3, \dots, P_n$. Forbind nu det sidste P_n med B og tegn gennem $P_1, P_2, P_3, \dots, P_n$ linjer parallelle med $P_n B$. Dette kan gøres med brug af passer og lineal ved at afsætte vinklen ved P_n i de andre punkter. Deres skæringspunkter med linjen l kalder vi for $Q_1, Q_2, Q_3, \dots, Q_n$, og disse punkter deler AB i n lige store dele:



Tilfældet $n = 5$



Tilfældet $n = 3$

Når dette er tilfældet, er det jo ikke en fjern tanke at rejse problemet om tredeling af en vinkel. Men det kunne mærkværdigvis ikke løses så let – ja det viste sig at være uløseligt. Men med flere hjælpemidler gik det fint.

4. Archimedes tredeling af vinklen

Archimedes lavede den nok enkleste konstruktion, hvor han brugte en »indskydningslineal«, dvs. en lineal med måleenheder. Han gjorde som følger:

<p>I enhedscirklen afsættes den vinkel, vi vil tredele, i 2. kvadrant (se figuren). Vi kalder vinklen $3v$, og ønsker altså at finde en vinkel af størrelse v. Vi tager nu linealen, lægger den, så den rører punktet A, således at vi får afsat et stykke BC, der har længden 1.</p>	
---	--

Det kan vi gøre ved at prøve os frem. Når BC er afsat, er trekantene OAB og OBC begge ligebenede, og ved at se på vinkelsummen finder vi vinklerne som vist på tegningen og specielt:

$$\square C = v,$$

altså netop en tredjedel af den, vi begyndte med.

Øvelse 6

Gennemfør beviset for at $\square C = v$.

I deres jagt på en løsning fandt de græske matematikere frem til en række nye, komplicerede kurver, som *Kvadratricen*, *Konkoiden*, *Arkimedes' spiral* og andre, som man i dag studerer under vektorfunktioner. Men ingen af dem kunne konstrueres med passer og lineal.

Gennem århundrederne fortsattes forsøgene, og mange troede, de havde fundet en løsning, som de så sendte til matematikere og videnskabelige akademier i håb om berømmelse og belønning. Det gik så vidt, at det franske Videnskabernes Akademi i 1775 udsendte en erklæring om, at det fremover hverken ville bedømme vinkeltredelinger, cirkelkvadraturer eller evighedsmaskiner.

I deres begrundelse skrev de, at der gik rygter om, at regeringer havde udlovet store dusører til dem, som løste problemerne, og at det var blevet til en sand galskab hos mange, som opgav deres arbejde og blev ganske forstyrrede i hovederne og i øvrigt ikke ville tage imod fornuft og acceptere, at de løsninger, de kom med, var fejlagtige.

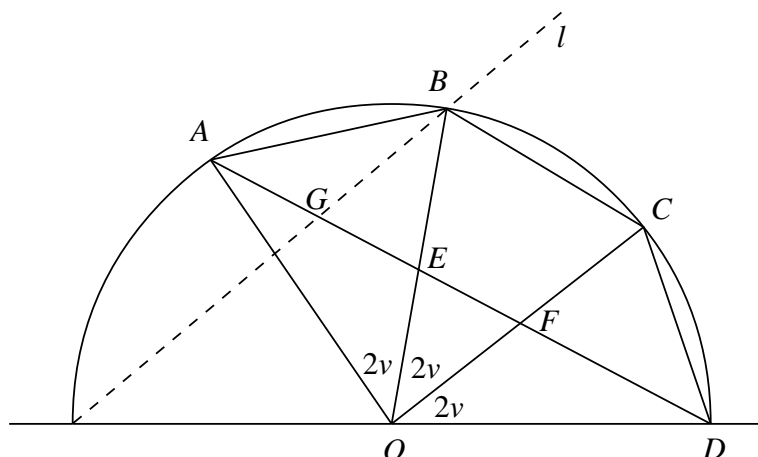
5. Oversættelse af vinkeltredeling til løsning af tredjegradslikning

Men det stoppede ikke de glade amatører, og mange lavede utroligt komplicerede konstruktioner, som var tæt ved, men aldrig eksakt løste opgaven. Således bragtes i årene omkring 1930 i et af de store tyske matematiktidsskrifter nogle artikler på grundlag af en skrædders ihærdige arbejde med passer og lineal.

Den første hed: »Die Winkeldreiteilung des Schneidermeister Kopf« og den næste: »Eine neue Winkeldreiteilung des Schneidermeister Kopf«.

Mere frugtbar var udviklingen blandt de arabiske matematikere omkring år 1000. De fandt frem til, at vinkeltredelingen kunne »oversættes« til et spørgsmål, om en bestemt *tredjegradslikning* havde en løsning. Dette blev senere fulgt op af Descartes (1596 – 1650), der i sin præsentation af koordinatsystemet behandlede kurver af tredje, fjerde og højere grad, for at vise den nye analytiske geometris overlegenhed. Descartes' argument var nogenlunde som følger:

Lad os igen kalde den vinkel, vi vil tredele, for $3v$, og begynde med at afsætte en vinkel på $6v$ i en enhedscirkel med centrum i O . De to punkter A og D forbindes, og vi antager nu, at vi kunne tredele vinklen på $6v$ for at *analysere* problemet nøjere. Tredeling af $6v$ ville give vinkler på $2v$ og punkterne B og C .



Trekantene OAB , OBC og OCD er alle ligebenede og har alle topvinklen $2v$, dvs. vinklerne ved grundlinjen er $90^\circ - v$, f.eks.

$$\sphericalangle A = \sphericalangle B = 90^\circ - v$$

Trekant OAD er også ligebenet, med topvinkel $6v$ og vinkler ved grundlinjen:

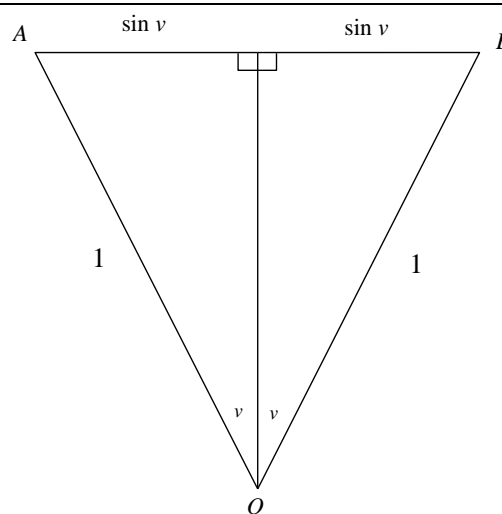
$$\sphericalangle OAD = \sphericalangle ODA = 90^\circ - 3v$$

Derfor ser vi, at i trekant ABE er $\sphericalangle EAB$ lig med $2v$, og da $\sphericalangle EBA = 90^\circ - v$, må også $\sphericalangle BEA$ være $90^\circ - v$, så trekanten er ligebenet og lignedannet med trekant OAB . Altså:

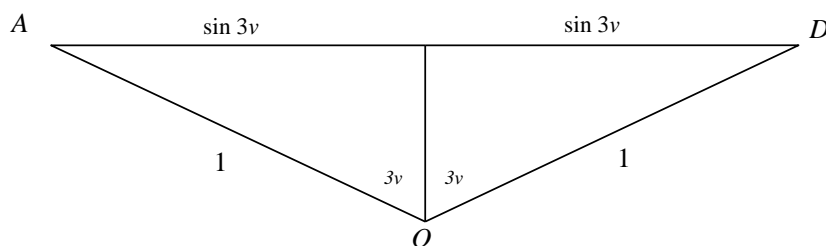
$$\frac{|AB|}{|AO|} = \frac{|BE|}{|AB|} \text{ eller } |BE| = \frac{|AB|^2}{|AO|} = |AB|^2, \text{ da } |AO| = 1.$$

Vores mål er at kunne konstruere $\sin(v)$ ud fra kendskab til $\sin(3v)$, for så kan vi også på enhedscirklen konstruere v ud fra $3v$.

Vi vil nå frem til dette ved at udnytte, at trekant OAB er ligebenet, så $|AB| = 2 \cdot \sin(v)$, se tegningen:



Samt udnytte, at trekant OAD er ligebenet, så $|AD| = 2 \cdot \sin(3v)$:



Nu mangler vi blot at få AD udtrykt ved AB . Vi vender tilbage til den samlede tegning:

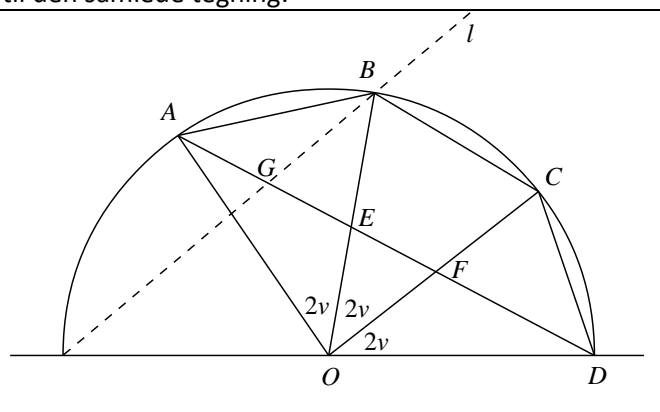
Vi trækker en linje l parallel med OC , og som skærer AD i G . Nu er $|BC| = |GF|$, og vi ved, at $|DF| = |DC| = |AB|$. Heraf ser vi, at $|AD| = |AE| + |DF| + |GF| - |GE| \Leftrightarrow |AD| = 3 \cdot |AB| - |GE|$

Se nu på trekant BGE . Den er konstrueret, så

$$\sphericalangle G = \sphericalangle F = 90^\circ - v$$

$\sphericalangle E$ er også lig med $90^\circ - v$. Men så er trekant BGE ligebenet og lignedannet med trekant ABE , dvs.

$$\frac{|GE|}{|BE|} = \frac{|BE|}{|AB|} \Leftrightarrow |GE| = \frac{|BE|^2}{|AB|}$$



Indsæt nu $|BE| = |AB|^2$:

$$|GE| = \frac{(|AB|^2)^2}{|AB|} = |AB|^3, \text{ dvs.}$$

$$|AD| = 3 \cdot |AB| - |GE| \quad \Leftrightarrow$$

$$|AD| = 3 \cdot |AB| - |AB|^3 \quad \Leftrightarrow$$

$$2 \cdot \sin(3v) = 3 \cdot 2 \cdot \sin(v) - (2 \cdot \sin(v))^3 \quad \Leftrightarrow$$

$$2 \cdot \sin(3v) = 6 \cdot \sin(v) - 8 \cdot \sin^3(v) \quad \Leftrightarrow$$

$$\sin(3v) = 3 \cdot \sin(v) - 4 \cdot \sin^3(v)$$

Hermed er tredelingen oversat til løsning af en tredjegradslikning: Givet tallet $\sin(3v)$. Find det x , der opfylder:

$$-4x^3 + 3x = \sin(3v)$$

Dette x er så $\sin(v)$, og kan på enhedscirklen give os v .

Eksempel

Tredeling af en vinkel på 30° . Vi ved, at $\sin(30^\circ) = \frac{1}{2}$. Altså findes $\sin(10^\circ)$ ud af ligningen:

$$-4x^3 + 3x = \frac{1}{2} \text{ eller } 8x^3 - 6x + 1 = 0$$

Det medførte ikke, at man nu kunne løse problemet med passer og lineal. Men oversættelsen fra et geometrisk til et algebraisk problem skulle vise sig at være et afgørende redskab til at bevise umuligheden af at løse opgaven.

6. Konstruerbare punkter – konstruerbare tal

I kapitel 1 viste vi, at man kan konstruere alle brøker, dvs hele \mathbb{Q} , samt en masse forskellige rod-udtryk. Men præcis hvilke? Det skal vi nu få styr på. Først:

6.1 Forudsætninger

Vi har givet et koordinatsystem med punkterne $P_1(0,0)$ og $P_2(1,0)$.

6.1.1 Tilladte konstruktioner med passer og lineal

- Givet to punkter, må vi tegne linjen gennem dem.
- Givet et punkt og en afstand (mellem to punkter), må vi tegne en cirkel med punktet som centrum og afstanden som radius.
- Ved hjælp af punkt 1 og 2 får vi konstrueret nye punkter ud fra givne punkter, nemlig:
 - skæringspunkter mellem linjer,
 - skæringspunkter mellem cirkler,
 - skæringspunkter mellem en cirkel og en linje.

Definition 1: Konstruerbare punkter

Mængden af alle de punkter i planen, der fremkommer ved at gå ud fra P_1 og P_2 og anvende de tilladte konstruktioner et endeligt antal gange, kalder vi for mængden af konstruerbare punkter.

6.2 Konstruktion af de konstruerbare punkter

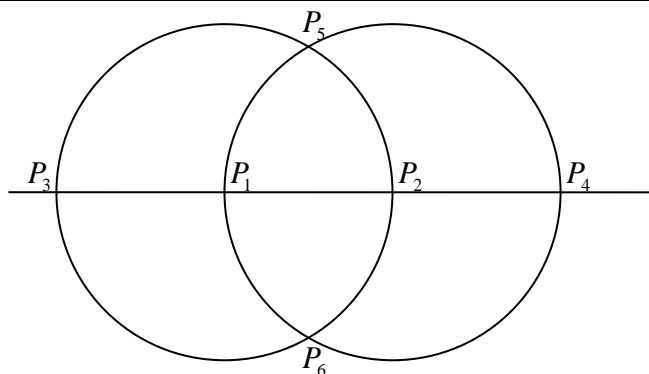
Mængden af konstruerbare punkter kan vi forestille os fremkomme ved skridt for skridt at køre punkt 1-3 igennem, ud fra de punkter, vi i det foregående skridt har skaffet os:

Forudsætninger $P_1(0,0)$ og $P_2(1,0)$.

1. skridt

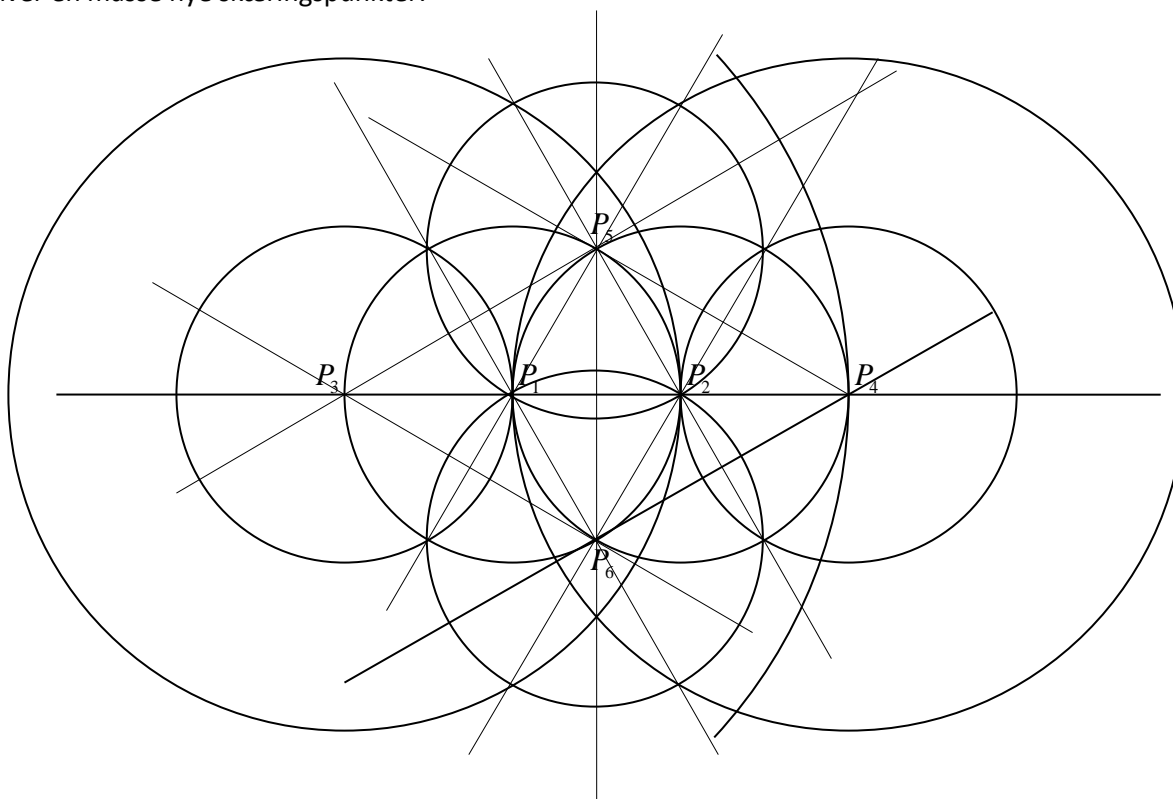
Vi har anvendt punkt 1 til at tegne den vandrette linje og punkt 2 til at tegne de to cirkler.

Det giver os 4 nye punkter som skæringspunkter mellem cirklerne og linjen og mellem cirklerne indbyrdes.



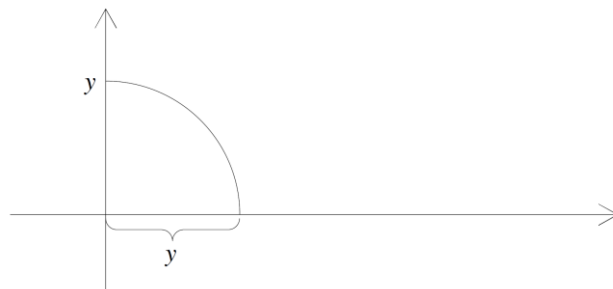
2. skridt

Nu har vi seks punkter og en nye afstande mellem forskellige af punkterne, der kan anvendes som radier i nye cirkler. Og det giver en masse nye skæringspunkter:



Vi stoppede midt i tegneriet, da det viste sig, at geometrien allerede her i 2. trin blev uoverskuelig.

Men skridt for skridt får vi fat i alle konstruerbare punkter. Et punkt repræsenteres af koordinater (x,y) . x og y findes ved at nedfælde en linje vinkelret på henholdsvis første- og andenaksen. Har vi et y på andenaksen, kan vi få det samme tal på førsteaksen ved at bruge passereren:



Definition 2: Konstruerbare tal

Koordinaterne til de konstruerbare punkter kaldes konstruerbare tal. Mængden af alle konstruerbare tal betegnes K .

Af vores undersøgelse i kapitel 1 kan vi nu drage følgende slutninger:

Sætning 1. Karakteristik af konstruerbare tal

1. $\mathbb{Q} \subseteq K$
2. Alle tal, der fremkommer ved at kombinere rationale tal ved hjælp af $+$, $-$, \cdot , $/$ og $\sqrt{\quad}$, er med i K .

7. Tallegemer

Vi vil nu nå frem til en mere overskuelig beskrivelse af K . Ovenstående tegning skulle være en rimelig begrundelse herfor. Sætningen ovenfor antyder det, vi vil nå frem til – nemlig at beskrive K som fremkommet ved at udvide \mathbb{Q} , først med almindelige kvadratrødder, så med kvadratrødder af kvadratrødder osv. osv.

For at holde styr på dette indføres først en definition af talmængder med særligt pæne egenskaber:

Definition 3

En talmængde L kaldes et *Legeme*, hvis der gælder følgende:

$$a, b \in L \Rightarrow a + b \in L$$

$$a \in L \Rightarrow -a \in L$$

$$a, b \in L \Rightarrow a \cdot b \in L$$

$$a, b \in L, b \neq 0 \Rightarrow \frac{a}{b} \in L$$

$$1 \in L$$

Kort og godt: Et legeme er en mængde L , hvori vi kan udføre de 4 regningsarter og stadig blive inden for L

Sætning 2: De rationale tal er det mindste tallegeme

1. \mathbb{Q} er et legeme.
2. \mathbb{Q} er det mindste legeme, dvs. ethvert tallegeme L må indeholde \mathbb{Q} .

Bevis selv punkt 1.

Bevis for punkt 2

Da $1 \in L$, får vi, at $2 = 1 + 1 \in L$, tilsvarende $3 \in L$, $4 \in L$ osv. Altså alle naturlige tal er med:

$$\mathbb{N} \subseteq L$$

Endvidere: $1 \in L \Rightarrow -1 \in L$, og derfor videre: $-2 \in L$, $-3 \in L$ osv., så alle negative hele tal er med i L . $1, -1 \in L \Rightarrow 1 + (-1) \in L$, dvs. $0 \in L$. Hermed har vi, at alle hele tal er med:

$$\mathbb{Z} \subseteq L$$

Divisionsreglen giver nu endelig, at for alle hele tal p og q , hvor $q \neq 0$, gælder: $p, q \in L \Rightarrow \frac{p}{q} \in L$.

Forhold mellem hele tal giver netop brøkerne, så:

$$\mathbb{Q} \subseteq L$$

Øvelse 7

Hvilke af følgende talmængder er legemer:

\mathbb{Q} , \mathbb{Z} , \mathbb{N} , \mathbb{R} , \mathbb{R}_+ , mængden af irrationale tal I ?

Sætning 3

Mængden af konstruerbare tal, K er et legeme.

Bevis

Følger umiddelbart af konstruktionerne i geometrisk algebra, hvor vi viser, at man kan lægge sammen og trække fra, gange og dividere med passer og lineal.

Prøv evt. selv at gå det efter.

Bemærkning: Normalt kan vi ikke uddrage rødder inden for et tallegeme. $\sqrt{2}$ er f.eks. ikke et rationalt tal. Vi kan uddrage rødder inden for \mathbb{Q} , og vi kan også inden for K (det beviste vi under geometrisk algebra).

Definition 4

Hvis $q \in \mathbb{Q}$ er et positivt rationalt tal, hvorom det gælder, at $\sqrt{q} \notin \mathbb{Q}$, så betegner $\mathbb{Q}(\sqrt{q})$ mængden af alle tal, der kan skrives som $a + b\sqrt{q}$:

$$\mathbb{Q}(\sqrt{q}) = \{a + b\sqrt{q} \mid a, b \in \mathbb{Q}\}$$

Sætning 4

$\mathbb{Q}(\sqrt{q})$ er et tallegeme, der indeholder \mathbb{Q} .

Tallegemet $\mathbb{Q}(\sqrt{q})$ kaldes en kvadratisk legemsudvidelse af \mathbb{Q} .

Først vises en hjælpesætning:

Hjælpesætning 5

Hvis $\sqrt{q} \notin \mathbb{Q}$, er opskrivningen af tal i $\mathbb{Q}(\sqrt{q})$ på formen $a + b\sqrt{q}$ entydig.

Bemærkning: $\mathbb{Q}(\sqrt{2})$ er alle tal på formen $a + b\sqrt{2}$, f.eks. $\frac{1}{2} - 2\sqrt{2}$ og $-\frac{7}{8} + \frac{2}{3}\sqrt{2}$. Hjælpesætningen siger altså, at et tal som $\frac{1}{2} - 2\sqrt{2}$ ikke kan skrives på denne form på andre måder. Et eksempel på noget, der ikke er entydig, er opskrivning af tal som produkter: $20 = 4 \cdot 5 = 2 \cdot 10$

Bevis

Påstanden er, at det samme tal *ikke* kan skrives på to forskellige måder på denne form. Dvs. hvis

$$x = a + b\sqrt{q} = c + d\sqrt{q}$$

så er $a = c$ og $b = d$.

Lad os derfor antage, at $a + b\sqrt{q} = c + d\sqrt{q}$.

Hvis nu $b = d$, får vi straks, at $a = c$, og så står der jo samme tal.

Hvis i stedet $b \neq d$, så omskriver vi:

$$a + b\sqrt{q} = c + d\sqrt{q} \Leftrightarrow$$

$$a - c = (b - d)\sqrt{q} \Leftrightarrow$$

$$\sqrt{q} = \frac{a - c}{b - d} \in \mathbb{Q}$$

Men vi havde jo forudsat, at $\sqrt{q} \notin \mathbb{Q}$, så det går ikke; altså kan det ikke gælde, at $b \neq d$.

Når $b = d$ gælder således også, at $a = c$. Og dermed har vi, at x ikke kan skrives på denne form på to forskellige måder.

Bemærkning

Specielt gælder: $a + b\sqrt{q} = 0 \Leftrightarrow a = 0 \wedge b = 0$

Bevis for sætning 4

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{q})$ er trivielt, da vi blot kan sætte $b = 0$.

Vi skal nu vise, at vi »kan regne indenfor $\mathbb{Q}(\sqrt{q})$ «. (I algebra bruger man også det udtryk, at $\mathbb{Q}(\sqrt{q})$ er lukket over for $+$, $-$, \cdot og $/$).

Lad os sige, at vi har to tal i $\mathbb{Q}(\sqrt{q})$:

$$x = a + b\sqrt{q} \text{ og } y = c + d\sqrt{q}$$

Så regner vi:

$$x + y = (a + b\sqrt{q}) + (c + d\sqrt{q}) = (a + c) + (b + d)\sqrt{q}$$

$$-x = -(a + b\sqrt{q}) = -a + (-b)\sqrt{q}$$

$$x \cdot y = (a + b\sqrt{q}) \cdot (c + d\sqrt{q}) = ac + bd(\sqrt{q})^2 + ad\sqrt{q} + bc\sqrt{q} = (ac + bdq) + (ad + bc)\sqrt{q}$$

$$y \neq 0, \frac{x}{y} = \frac{a + b\sqrt{q}}{c + d\sqrt{q}} = \frac{(a + b\sqrt{q})(c - d\sqrt{q})}{(c + d\sqrt{q})(c - d\sqrt{q})} = \frac{(ac - bdq) + (bc - ad)\sqrt{q}}{(c^2 - (d\sqrt{q})^2)} = \frac{ac - bdq}{c^2 - qd^2} + \frac{bc - ad}{c^2 - qd^2} \cdot \sqrt{q}$$

Alle fire udregninger ender på formen

$$r_1 + r_2\sqrt{q}, r_1, r_2 \in \mathbb{Q},$$

netop fordi \mathbb{Q} selv er et tallegeme.

De tre første er simple omskrivninger.

I den sidste forlængede vi med $c - d\sqrt{q}$ for at udnytte reglen

$$(a + b)(a - b) = a^2 - b^2$$

og dermed få \sqrt{q} væk i nævneren.

Vi ved, at $c - d\sqrt{q} \neq 0$, for hvis der gjaldt, at $c - d\sqrt{q} = 0$, så var $c = 0$ og $d = 0$, og dermed ville også $y = c + d\sqrt{q}$ være 0. Men vi har netop forudsat, at $y \neq 0$.

Ovenstående definitioner og sætninger er ikke specielle for \mathbb{Q} . Vi har kun brugt, at \mathbb{Q} er et tallegeme. Derfor kan vi formulere resultaterne mere generelt:

Definition 5

Hvis L er et tallegeme, og q er et tal i L , således at $\sqrt{q} \notin L$, defineres $L(\sqrt{q})$ som

$$L(\sqrt{q}) = \{a + b\sqrt{q} \mid a, b \in L\}$$

Sætning 6

1. Opskrivningen af tal i $L(\sqrt{q})$ på formen $x = a + b\sqrt{q}$, $a, b \in L$, er entydig.
2. $L \subseteq L(\sqrt{q})$, og $L(\sqrt{q})$ er selv et tallegeme.

Bemærkning: $L(\sqrt{q})$ kaldes derfor et *udvidelseslegeme* til L . Inden for algebra siger man også, at $L(\sqrt{q})$ er fremkommet ved *adjunktion* af \sqrt{q} til L .

8. Beskrivelse af de konstruerbare tal

Vi er nu i stand til at beskrive K – de konstruerbare tal – ved hjælp af udvidelseslegemer til \mathbb{Q} .

1. Først vender vi lige tilbage til konstruktionen af alle de konstruerbare punkter. Uanset hvor uoverskuelig en tegning kunne være, er det alligevel klart, at der *i hvert skridt* kun bliver konstrueret et bestemt, *endeligt* antal punkter.

Derfor kan vi fortsætte den nummerering af dem, som begyndte med P_1, P_2, \dots, P_6 , så vi får en følge af punkter:

$$P_1, P_2, \dots, P_n$$

Det er ligegyldigt, hvilken rækkefølge vi vælger inden for hvert skridt.

Ud fra punkterne får vi så de konstruerbare tal, som tilsvarende kan skrives op i rækkefølge:

$$x_1, x_2, \dots, x_n \quad (*)$$

Det er ligegyldigt, hvilken rækkefølge vi vælger inden for hvert skridt. Det eneste af betydning er, at *alle er med*, samt at vi først tager alle fra første skridt, dernæst alle fra andet skridt osv.

2. Dernæst går vi i gang med at konstruere en følge af udvidelseslegemer til \mathbb{Q} efter følgende recept: Vi bevæger os frem i følgen af x 'er, til vi første gang møder et x_i , hvor $x_i \notin \mathbb{Q}$. Efter en opskrift, der følger nedenfor i punkt 3, finder vi så et tal $l_0 \in \mathbb{Q}$ og danner $L_1 = \mathbb{Q}(\sqrt{l_0})$.

Nu har vi begyndelsen på følgen, som vi leder efter, idet L_1 er et legeme, og $\mathbb{Q} \subseteq L_1$.

Vi fortsætter frem i rækken af x 'er, til vi første gang møder et x_j , hvor $x_j \notin L_1$, finder et $l_1 \in L_1$ efter opskriften nedenfor og danner som før $L_2 = L_1(\sqrt{l_1})$.

Nu gælder derfor:

$$\mathbb{Q} \subseteq L_1 \subseteq L_2,$$

og processen fortsætter, så vi får konstrueret en følge af *udvidelseslegemer*:

$$\mathbb{Q} \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \dots \subseteq L_k$$

3. Det eneste, vi mangler at angive, er, hvorledes vi finder de $l_0, l_1, l_2, l_3, \dots, l_k$, som anvendes ved hver udvidelse:

$$L_{k+1} = L_k(\sqrt{l_k}), \text{ hvor } l_k \in L_k$$

Lad os sige, vi er nået til konstruktionen af L_k og skal videre. Vi går som beskrevet frem i rækken og når frem til et x_n . Lad os nu lige overveje, hvorledes et sådant x_n i rækken af konstruerbare tal fremkommer. Der er tre mulige måder – som skæringspunkt:

- I. mellem to linjer,
 - II. mellem en linje og en cirkel,
 - III. mellem to cirkler,
- hvor disse linjer og cirkler alle er fastlagt ud fra nogle af de foregående punkter, dvs. ud fra nogle af x_1, x_2, \dots, x_{n-1}

En linje fastlagt af punkterne (x_i, y_i) og (x_j, y_j) har ligningen:

$$y - y_j = \frac{y_i - y_j}{x_i - x_j} \cdot (x - x_j),$$

og skrives dette på formen

$$ax + by + c = 0,$$

er det let at se, at a , b og c er fremkommet af de foregående tal ved brug af regnearterne $+$, $-$, \cdot og $/$. Altså: $a, b, c \in L_k$.

En cirkel med centrum i (x_k, y_k) og radius r (som er et tal fastlagt ud fra de foregående punkter), har ligningen:

$$(x - x_k)^2 + (y - y_k)^2 = r^2,$$

og skrives denne på formen:

$$x^2 + y^2 + dx + ey + f = 0,$$

ses let, at d , e og f alle er fremkommet af de foregående punkter ved brug af $+$, $-$, \cdot og $/$. Altså:

d , e og f ligger også i L_k .

Vi ser nu på de tre nævnte tilfælde:

- I. x_n stammer fra et skæringspunkt mellem to linjer:

$$a_1x + b_1y + c_1 = 0$$

$$a_2x + b_2y + c_2 = 0$$

x_n findes altså ved at løse disse to ligninger og må derfor fremkomme af a 'erne, b 'erne og c 'erne ved brug af $+$, $-$, \cdot og $/$. Men så ligger x_n jo selv i L_k . Med andre ord bidrager x_n ikke med noget nyt i dette tilfælde: L_k bliver ikke udvidet.

- II. x_n stammer fra et skæringspunkt mellem

linjen: $ax + by + c = 0$

og cirklen: $x^2 + y^2 + dx + ey + f = 0$

a og b kan ikke begge være lig nul. Lad os sige $b \neq 0$. Så findes y af den første ligning:

$$y = -\frac{ax + c}{b},$$

som dernæst indsættes i den anden ligning:

$$x^2 + \left(-\frac{ax + c}{b}\right)^2 + dx + e \cdot \left(-\frac{ax + c}{b}\right) + f = 0$$

Vi kan se, at denne ligning kan reduceres til en ligning af formen:

$$Ax^2 + Bx + C = 0, \quad A, B, C \in L_k$$

Vi ved jo, at $x = x_n$ er en løsning. Derfor vil vi opskrive løsningsformlen:

$$x_n = \frac{-B + \sqrt{D}}{2A} \vee x_n = \frac{-B - \sqrt{D}}{2A}, \quad \text{hvor } D = B^2 - 4AC \in L_k.$$

Hvis $\sqrt{D} \in L_k$, vil også $x_n \in L_k$ og bidrager således heller ikke til noget nyt; L_k bliver ikke udvidet. Men hvis $\sqrt{D} \notin L_k$, så sætter vi:

$$L_{k+1} = L_k(\sqrt{D}), \text{ dvs. } D \text{ er det omtalte tal } l_k.$$

III. x_n stammer fra et skæringspunkt mellem to cirkler:

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0$$

$$x^2 + y^2 + d_2x + e_2y + f_2 = 0$$

Ved at trække den nederste fra den øverste får vi omformet dette ligningssystem til følgende to ligninger:

$$(d_1 - d_2)x + (e_1 - e_2)y + (f_1 - f_2) = 0$$

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0$$

Men det er jo præcis samme situation som under punkt II med en linje og en cirkel, så det har vi allerede behandlet.

Konklusion: Et nyt tal i rækken af konstruerbare tal vil enten blot være en kombination af de foregående tal ved brug af +, -, · og /, dvs. ligge indenfor det tallegeme, som de hidtidige tal tilhører. Eller der vil findes et $l_k \in L_k$, så x_n ligger i $L_k(\sqrt{l_k})$, som så bliver det næste i følgen af tallegemer.

Sætning 7

Hvis K er mængden af konstruerbare tal, og L_k har samme betydning som ovenfor, så gælder:

$$K = \bigcup_{k=1}^{\infty} L_k$$

Bevis

Lighedstegnet mellem de to mængder vises ved en almindelig anvendt teknik, nemlig:

$$1. K \subseteq \bigcup_{k=1}^{\infty} L_k$$

$$2. K \supseteq \bigcup_{k=1}^{\infty} L_k,$$

for så må de jo være ens.

1. L_k 'erne er konstrueret, så ethvert $x_n \in K$ bliver fanget og kommer med i et eller andet L_k .

$$\text{Derfor er } K \subseteq \bigcup_{k=1}^{\infty} L_k.$$

2. Se på følgen:

$$\square \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \dots \subseteq L_k$$

Vi ved, at $\square \subseteq K$. L_1 består af tal af formen $a + b\sqrt{l_0}$, $a, b, l_0 \in \square$. Fra sætning 3, side 8, ved vi, at $\sqrt{l_0} \in K$ og derfor også, at $b\sqrt{l_0} \in K$ og endelig, at $a + b\sqrt{l_0} \in K$. Altså:

$$L_1 \subseteq K$$

L_2 består af tal af formen $a + b\sqrt{l_1}$, $a, b, l_1 \in L_1 \subseteq K$. Som før ved vi derfor også, at $\sqrt{l_1} \in K$ og derfor også, at $b\sqrt{l_1} \in K$ og endelig, at $a + b\sqrt{l_1} \in K$. Altså:

$$L_2 \subseteq K$$

Dette kan vi indlysende nok fortsætte og får for ethvert k , at $L_k \subseteq K$, altså:

$$K \supseteq \bigcup_{k=1}^{\infty} L_k,$$

og sætningen er vist.

9. Tredeling af en vilkårlig vinkel er ikke mulig

Vi er nu endelig parat til at vise umuligheden af at tredede en vilkårlig vinkel, dvs umuligheden af at konstruere en sådan tredeling med passer og lineal.

Først vises følgende vigtige sætning, der også har almen interesse:

Sætning 8: Hvis et tal er en rod er også partneren en rod

Lad $L(\sqrt{q})$ være et udvidelseslegeme til et tallegeme L , og lad

$$P(x) = a_n x^n + \dots + a_1 x + a_0$$

være et polynomium med koefficienter i L : $a_n, \dots, a_1, a_0 \in L$. Så gælder:

Hvis $a + b\sqrt{q}$ er en rod i $P(x)$, så er også $a - b\sqrt{q}$ en rod i $P(x)$.

$a - b\sqrt{q}$ kaldes *partneren* til $a + b\sqrt{q}$.

Bemærkning Prøv selv at overveje situationen, hvor $P(x)$ er et andengradspolynomium med rationale koefficienter (tænk på løsningsformlen).

Bevis

Først en betegnelse: Hvis $x = a + b\sqrt{q}$, betegner vi partneren med \bar{x} :

$$\bar{x} = a - b\sqrt{q}$$

Partneren til et tal $a \in L$ er tallet selv, for her gælder jo, at $b = 0$:

$$\bar{a} = a$$

Dernæst en iagttagelse: Hvis $x = a + b\sqrt{q}$, $y = c + d\sqrt{q}$, har vi tidligere udregnet

$$x \cdot y = (ac + bdq) + (ad + bc)\sqrt{q}.$$

Tilsvarende kan vi udregne

$$\bar{x} \cdot \bar{y} = (a - b\sqrt{q}) \cdot (c - d\sqrt{q}) = (ac + bdq) - (ad + bc)\sqrt{q}.$$

Men heraf ser vi, at

$$\overline{x \cdot y} = \bar{x} \cdot \bar{y}$$

Dette kan vi naturligvis fortsætte, så vi også får

$$\overline{x^n} = (\bar{x})^n.$$

Det er endvidere let at se, at

$$\overline{x + y} = \bar{x} + \bar{y}.$$

Nu kan vi indse sætningens rigtighed: Lad nemlig $x_0 = a + b\sqrt{q}$ være en rod i $P(x)$:

$$P(x_0) = 0 \text{ eller } a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_1 x_0 + a_0 = 0$$

Tag nu partneren på begge sider:

$$\overline{a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_1 x_0 + a_0} = \bar{0} = 0$$

Anvend de regneregler, vi netop har indset, til omskrivning af venstre side:

$$\overline{a_n x_0^n} + \overline{a_{n-1} x_0^{n-1}} + \dots + \overline{a_1 x_0} + \overline{a_0} = 0 \quad \Leftrightarrow$$

$$\overline{a_n (x_0)^n} + \overline{a_{n-1} (x_0)^{n-1}} + \dots + \overline{a_1 x_0} + \overline{a_0} = 0 \quad \Leftrightarrow$$

$$a_n (\overline{x_0})^n + a_{n-1} (\overline{x_0})^{n-1} + \dots + a_1 \overline{x_0} + a_0 = 0$$

Men venstre side er jo nu $P(\overline{x_0})$, så der står

$$P(\overline{x_0}) = 0,$$

altså at også $\overline{x_0}$ er en rod.

Hjælpesætning 9

Lad $L(\sqrt{q})$ være et udvidelseslegeme af L . Sæt:

$$P(x) = x^3 - 3x + 1$$

Så gælder, at hvis $P(x)$ har en rod i $L(\sqrt{q})$, så har $P(x)$ også en rod i L .

Bemærkning. Slå tilbage til kapitel 5, *Oversættelse af vinkeltredeling til løsning af tredjegradslikning* og find hvad det var for et polynomium, der dukkede op, da vi undersøgte, om en vinkel på 30° kunne tredeles. Det ligner meget $P(x)$, og det er da også begrundelsen for at vise denne ellers ret uinteressante sætning.

Bevis

Lad $x_0 = a + b\sqrt{q}$, $a, b, q \in L$, være en rod i $P(x)$.

Hvis $b = 0$, vil x_0 være lig med a . Og så er det jo trivielt, at $P(x)$ har en rod (nemlig x_0) i L .

Hvis $b \neq 0$, så er ifølge sætning 12 partneren $\overline{x_0} = a - b\sqrt{q}$ også en rod i $P(x)$, og der gælder:

$$x_0 \neq \overline{x_0}$$

Ved polynomiers division kan vi derfor få $P(x)$ skrevet således:

$$P(x) = (x - (a + b\sqrt{q}))(x - (a - b\sqrt{q}))(x - c),$$

hvor c er den tredje rod i $P(x)$.

Når vi ganger parenteserne på højre side ud, skal vi få venstresiden. På venstre side er der $0x^2$, hvilket der derfor også må være på højre side. Lad os se efter og finde, hvor mange x^2 der er:

$$-c \cdot x^2 - (a + b\sqrt{q}) \cdot x^2 - (a - b\sqrt{q}) \cdot x^2 = (-c - (a + b\sqrt{q}) - (a - b\sqrt{q})) \cdot x^2,$$

som altså er lig med $0x^2$. Men det vil jo sige:

$$-c - (a + b\sqrt{q}) - (a - b\sqrt{q}) = 0 \Leftrightarrow -c - 2a = 0 \Leftrightarrow c = -2a$$

Hermed har vi vist, at $P(x)$ har en rod i L , nemlig:

$$c = -2a \in L$$

Dernæst vises:

Hjælpesætning 10

$P(x) = x^3 - 3x + 1$ har ingen rationale rødder.

Bevis

Lad os sige, det rationale tal r var en rod i $P(x)$, og lad os sige, r var skrevet som en uforkortelig brøk:

$$r = \frac{p}{q}$$

Så gjaldt der:

$$\left(\frac{p}{q}\right)^3 - 3\frac{p}{q} + 1 = 0 \Leftrightarrow \frac{p^3}{q^3} - 3\frac{p}{q} + 1 = 0 \Leftrightarrow p^3 - 3pq^2 + q^3 = 0$$

I denne ligning isolerer vi først q^3 , dernæst p^3 og får de to ligninger:

$$1. p^3 = 3pq^2 - q^3$$

$$2. -p^3 + 3pq^2 = q^3$$

Af 1. ser vi, at det hele tal q går op i højresiden, derfor også i venstresiden.

Men $\frac{p}{q}$ var jo uforkortelig, så den eneste mulighed for q er at være $+1$ eller -1 .

Af 2. ser vi på samme måde, at p må være enten $+1$ eller -1 . Derfor er tallet r enten $+1$ eller -1 .

Altså: $r = +1$ og $r = -1$ er de eneste mulige rationale rødder. Om de nu også virkelig dur, kan vi efterprøve ved blot at indsætte dem og se efter. Prøv at gøre det og se, at de faktisk ikke dur. Altså: *der er ingen rationale rødder.*

Hovedsætning 11

Det er umuligt at tredele en vilkårlig vinkel med passer og lineal.

Bemærkning: Vi husker, at nogle vinkler naturligvis kan tredeles. Når vi kan konstruere en vinkel på 30° ved f.eks. at halvere en vinkel på 60° (som vi får fra en ligesidet trekant), ja så kan vi jo sige, at vi har tredelt en vinkel på 90° . Det, sætningen siger, er, at vi ikke kan tredele en vilkårlig vinkel. Dette bevises ved at vise, at en ganske bestemt vinkel, nemlig den på 30° ikke kan tredeles.

Bevis

Vi viser, at en vinkel på 10° ikke er konstruerbar, ved at vise, at tallet $\sin(10^\circ)$ ikke er et konstruerbart tal (det er jo 1. koordinaten til retningspunktet P_{10} på enhedscirklen).

Der gælder følgende ligning (se side 6 i kapitel 5) for enhver vinkel u :¹

$$\sin(3u) = -4\sin^3(u) + 3\sin(u),$$

og idet vi sætter $u = 10^\circ$, får vi, som vi også så på side 6:

$$\sin(30^\circ) = -4\sin^3(10^\circ) + 3\sin(10^\circ) \Leftrightarrow$$

$$\frac{1}{2} = -4\sin^3(10^\circ) + 3\sin(10^\circ) \Leftrightarrow$$

$$8\sin^3(10^\circ) - 6\sin(10^\circ) + 1 = 0$$

Nu substitueres $x = 2\sin(10^\circ)$, så ligningen bliver til $x^3 - 3x + 1 = 0$, som vi kender fra sætningen ovenfor. Derfor ser vi nu: Hvis $\sin(10^\circ)$ var konstruerbar, var også $2\sin(10^\circ)$ det. Dermed ville polynomiet $P(x) = x^3 - 3x + 1$ have en konstruerbar rod, x_0 .

Da $x_0 \in K$, vil der findes et L_k så $x_0 \in L_k$. Hjælpesætning 14 giver derfor:

$P(x)$ har en rod i $L_k = L_{k-1}(\sqrt{I_{k-1}}) \Rightarrow P(x)$ har en rod i L_{k-1} .

¹Strengt taget har vi kun vist, at formlen gælder for vinkler, hvor $6^\circ \leq \nu \leq 180^\circ$, dvs. for $\nu \leq 30^\circ$. Men det kan vises, at trigonometriske formler, der gælder i et interval, uanset hvor lille, gælder overalt! Vi benytter imidlertid her kun det, vi har vist.

Som vi gjorde tidligere, kan vi også her fortsætte dette nedad og får: $P(x)$ har en rod i $L_k \Rightarrow P(x)$ har en rod i $L_{k-1} \Rightarrow P(x)$ har en rod i $L_{k-2} \Rightarrow \dots \Rightarrow P(x)$ har en rod i \mathbb{Q} .

Men det har $P(x)$ ikke, ifølge hjælpesætning 15. Derfor har $P(x)$ overhovedet ikke nogen konstruerbare rødder, altså $\sin(10^\circ)$ er ikke konstruerbar: Vinklen på 30° kan ikke tredeles.

Og således fandt det gamle græske problem sin løsning med hjælp fra moderne algebra

10. Litteraturliste

- Anglig & Lambek, *The Heritage of Thales*, Springer, 1995. (En matematikhistorie, hvor sætningerne faktisk bevises fuldt ud, f.eks. om umuligheden af vinklens tredeling).
- E.T. Bell, *Matematikkens mænd*, Reitzel, 1944.
- Burtons *History of Mathematics*, Brown Publishers, 1995. (Indeholder et kapitel med en række større øvelser om de klassiske konstruktionsopgaver).
- Flemming Clausen og Jørgen Falkesgaard, *Tal og Tanke*, Munksgaard, 1985.
- Poul la Cour, *Historisk matematik*, Rosenkilde og Bagger, 1961.
- Euklid, *Elementer I – IV*, Trips forlag. (Fotografisk genoptryk af Thyra Eibes oversættelse fra 1897).
- Howard Eves, *Introduction to the History of Mathematics*, The Saunders, 1992. (Indeholder et kapitel med en række større øvelser om de klassiske konstruktionsopgaver).
- Thomas Heath, *A History of Greek Mathematics, vol I*, Dover, 1981. (Standardværket – fotografisk genoptryk. Værket er meget detaljeret om alle spørgsmål. Er tro mod de græske matematikers argumentation).
- Herodot, *Historien*, Gyldendal, 1975.
- Viktor Katz, *A History of Mathematics*, Harper Collins, 1993. (En matematikhistorie, hvor argumentationen for de matematiske sætninger gengives detaljeret og i respekt for de originale metoder, samtidig med at læsevenligheden er prioriteret).
- Jesper Lützen, *Cirkelns kvadratur, Vinklens tredeling, Terningens fordobling*, Systime, 1985.
- Preben Vestergaard, *Løste og uløste matematiske problemer*, Aalborg Universitetsforlag, 1983.
- Hans Wussing, *Biographien Bedeutender Mathematiker*, Berlin, 1975.
- *Vinklens tredeling*, et matematikprojekt af Karen Birkelund og Bjørn Christensen, IMFUFA skrifter nr. 230, 1992.

11. Tillæg. Om Galois' korte liv og bratte død

Selv om en del store matematikere (især Lagrange, 1736 – 1813) havde arbejdet med at udvikle en sådan ny algebra, tilkommer æren den geniale franske matematiker Evariste Galois. Efter ham kaldes denne del af algebraen, der viste sig at have de mest forskelligartede og overraskende anvendelser, for *Galois' teori*.

Galois' liv var som en klassisk græsk tragedie. Han blev født i 1811, hvor hele Europa var revet op af Napoleonskrigene, og Frankrig selv splittet på kryds og tværs af modsætningerne mellem demokraterne, der ville forsvare idealerne fra den store revolution i 1789, og monarkister af mange afskygninger.

Den meget temperamentsfulde Evariste Galois tog allerede fra gymnasietiden aktivt del i agitationen for at få genetableret republikken, og med sine indlæg i gymnasieblade og taler på møder og værtshuse bragte han sig i konflikt med myndighederne.

I juli 1830 forsøgte kongen, der var blevet indsat efter Napoleons fald, at bremse den demokratiske bevægelse med censur og beslaglæggelse af trykkerierne; men det blev i stedet signal til oprør. Det var i øvrigt på samme tid, at nationale konflikter og frihedskrige førte til, at Belgien rev sig løs fra Holland og kom på Europakortet, Serbien blev selvstændig, og Grækenland endelig fik smidt tyrkerne ud og efter næsten 2000 år igen blev herrer i deres eget hus.

I Paris lykkedes det godt nok at få væltet kongen, som flygtede til England; men i stedet for den demokratiske republik blev der indsat en ny, men dog mere liberal konge. Republikanerne – og blandt dem Evariste Galois og de andre studenter, som var højlydt utilfredse – fortsatte deres agitation, men måtte nu opleve at myndighederne skred hårdt ind.

Efter at have skrevet et læserbrev vendt mod sin rektor, blev Galois smidt ud af skolen i december 1830. Han sluttede sig til republikanergarden, der er de mest oprørske, og som kort efter forbydes. Da Galois selv offentligt udtaler sig imod kongen, fængsles han i maj 1831.

Han løslades for en kort bemærkning i juni, men ryger ind igen i juli 1831, efter at han har deltaget i en demonstration på Bastilledagen (14. juli – årsdagen for den store revolution i 1789). 29. april 1832 slipper han endelig ud.

Ude af fængslet opdager han, at der er en medbejler til den pige, han er forelsket i. Straks udfordrer den temperamentsfulde Galois den anden til duel, men er tilsyneladende klar over sine ringe chancer, for om natten til den 30. maj, hvor duellen skal finde sted, samler han febrilsk sine matematiske artikler og udkast sammen og skriver en længere redegørelse for, at han her har udviklet en helt ny algebraisk teori, der vil have vide anvendelsesmuligheder (og bl.a. demonstrere umuligheden af at løse de tre klassiske problemer).

Redegørelsen var især beregnet for den store tyske matematiker Gauss (1772 – 1855). Galois skriver:

»[...] jeg har gjort nogle nye opdagelser i analysen. [...] Bed Jacobi eller Gauss om offentligt at udtale deres mening, ikke om sandheden, men om betydningen af disse sætninger. Senere vil der, håber jeg, findes matematikere, som vil have fordel af at dechifrere alt dette rod [...]«

Og i papirerne kradsede han flere steder ned: »jeg har ikke tid, jeg har ikke tid.«

Den 30. maj 1832 om morgenen blev Evariste Galois, som han havde forudanet, dødeligt såret i duellen; han blev efterladt med sine skudsår og først fundet en del timer senere af en bonde, der bragte ham til et nærliggende hospital, men for sent. Han overlevede ikke.

Og hans papirer nåede tilsyneladende aldrig frem til Gauss. Uheldet syntes at forfølge stakkels Galois efter hans død, som det var sket, mens han levede.

Artiklerne var i forskellige versioner sendt frem til tidsskrifter og bedømmelse hos kendte matematikere. En af disse, Cauchy (1789 – 1857) havde med interesse læst noget af det, men blev uheldigvis syg, da han skulle præsentere Galois' ideer for Akademiet i 1829. Samme år dumper Galois selv ved optagelsesprøven til Polyteknisk læreanstalt, da han er stærkt nedbrudt over, at hans far efter en smædekampagne havde begået selvmord få dage før prøven.

I 1830 vender Cauchy så tilbage til Galois og beder ham om at omskrive materialet til en prisopgave, som akademiet netop havde udskrevet. Men da Galois gør det og indsender sin nye version, bliver hans bidrag væk! Sandsynligvis fordi komitéformanden Fourier (1768 – 1830, kendt fra teorien om Fourier-rækker, der anvendes i studiet af sammensatte harmoniske svingninger) havde taget artiklen med hjem, og pludselig dør.

Et af de andre komitemedlemmer er Poisson (1781 – 1840, kendt fra Poisson-fordelingen, der anvendes i sandsynlighedsregning og statistik) anmoder nu Galois om igen at lave en ny version, denne gang med eksempler på de rige anvendelsesmuligheder, hans teori har. Artiklen indleveres først på året 1831; men i juli 1831 afviser Poisson den med bemærkningen »uforståelig«.

Ad mærkelige omveje lander Galois' artikler og sidste breve i 1843 hos endnu en af Frankrigs mange store matematikere, Liouville (1809 – 1882, især kendt fra differentialligningsteorien), og endelig er der en, som forstår teoriens betydning og genialitet. Han bearbejder det, og i 1846 offentliggøres materialet.

Sideløbende hermed havde Gauss og andre udviklet elementer af den nye algebraiske teori, som smeltede sammen med Galois' bidrag til det, vi i dag blot kalder for *Algebra*, og hvor teorien om *grupper*, om *legemer* og *Galois' teori* er specielle områder.